THE TAXBOOK News
Release Date: 12/12/2018

W-2 Scams

Cross References

- IR-2018-243, December 6, 2018

The IRS is once again warning taxpayers, employers, and tax professionals to be on guard against the latest wave of W-2 scams. This has become one of the more dangerous email scams for tax administration. The emails appear to be from an executive or organization leader to a payroll or human resources employee. It may start with a simple, "Hey, you in today?" By the end of the exchange, all the organization's Forms W-2 for their employees may be in the hands of cybercriminals. This puts workers at risk for tax-related identity theft.

Because payroll officials believe they are corresponding with an executive, it may take weeks for someone to realize a data theft has occurred. Generally, the criminals are trying to quickly take advantage of their theft, sometimes filing fraudulent tax returns within a day or two. This scam is such a threat to taxpayers that a special IRS reporting process has been established.

The following is an abbreviated list of how to report these schemes:

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide contact information. In the subject line, type "W2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information data.
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3.gov). Businesses/payroll service providers may be asked to file a report with their local law enforcement agency.
- Notify employees so they may take steps to protect themselves from identity theft. The Federal Trade Commission's www.identitytheft.gov provides guidance on general steps employees should take.
- Forward the scam email to phishing@irs.gov.

Employers are urged to put steps and protocols in place for the sharing of sensitive employee information such as Forms W-2. One example would be to have two people review any distribution of sensitive W-2 data or wire transfers. Another example would be to require a verbal confirmation before emailing W-2 data. Employers also are urged to educate their payroll or human resources departments about these scams.